Council of the
European Union

Brussels, 15 January 2021
(OR. en)

5157/21

CSC 6
RELEX 10

NOTE

From:	General Secretariat of the Council
To:	Coordination Committee for Communication and Information Systems (CCCIS)
Subject:	Budgetary planning for a secure videoconferencing system (sVTC) for the European Council and the Council

I. Purpose

1. This document sets out the budgetary implications of deploying, accrediting and operating a secure videoconferencing system for the European Council and the Council. It provides an preliminary planning roadmap for the various phases of designing and deploying system.

II. General remarks

2. In analysing the budgetary requirements for a secure videoconferencing system, the GSC has not taken into account the cost savings of not holding a physical meeting, as they are often intangible (urgency, time savings), and spread over numerous cost centres inside and outside the GSC (general secretariat, host country security and protocol services, transport costs, member state expenses). Estimates have put the total cost for a two-day leaders' meeting at well over 1 million Euros.

3. Estimates have had to be used for the cost of certain components, as the detailed system design has not yet been completed, and some costs depend on the outcome of procurement procedures still to be launched. The estimates of equipment and services provide for a certain safety margin, which have been transparently indicated in the budget evaluation.

4. The budgetary planning does not include the following costs:

- Staffing costs in the GSC and member states during project phases 1 and 2 (requirements and build phases) have not been included. In phase 3 the marginal costs of operators in the GSC have been included;

- Communication costs are excluded. It is envisaged that internet connectivity will be used, as is the case with other high classified systems for EUCI the GSC is currently developing and deploying;

- Physical works in the GSC or at the endpoint locations in member states or the Commission or EEAS are not included. These locations need to be properly designed and built to meet requirements in the Council Decision on security rules for protecting EU classified information. **It will be for each member state to make provision for the necessary security works to enable proper accreditation of the system for use by leaders and ministers for discussing EU classified information.** The GSC expertise, in having a formal Tempest Authority, may advise member states in setting out their physical implementations.

Budget table

5. The following table gives an overview of identified costs (both investment and operating costs) to be borne by the Council budget for the secure videoconferencing system.

	Investment	Risk margin	Investment +Risk	Maintenance	Recurring	Quantity	Total	
							Investment	Recurring
Member States sites								
Crypto-S	€ 6,000	1.5	€ 9,000	20%	€ 1,800	90	€ 810,000	€ 162,000
VTC - Room equipment	€ 5,000	1.5	€ 7,500	10%	€ 750	90	€ 675,000	€ 67,500
Installation	€ 4,000	1.2	€ 4,800			90	€ 432,000	
Central location								
Crypto-S	€ 6,000	1.5	€ 9,000	20%	€ 1,800	4	€ 36,000	€ 7,200
VTC - Room equipment	€ 50,000	1.5	€ 75,000	10%	€ 7,500	2	€ 150,000	€ 15,000
VTC - Licenses					€ 50,000	1		€ 50,000
VTC - Servers	€ 50,000	1.5	€ 75,000	10%	€ 7,500	1	€ 75,000	€ 7,500
Installation	€ 50,000	1.5	€ 75,000			1	€ 75,000	
Operators					€ 50,000	2		€ 100,000
Accreditation Process	€ 100,000	1.5	€ 150,000			1	€ 150,000	
						Grand Total:	**€ 2,403,000**	**€ 409,200**

6. The budget covers the cost of investing in and initial operation of the central hub managed by the GSC, as well as the equipment (both the cryptographic products and endpoint hardware) to be deployed at two endpoints in each Member State and in the Commission, the EEAS and the GSC.

7. Regarding central hub housed in the GSC:

- software licenses, crypto equipment and on-site servers will be installed in the GSC's secure data centre for classified systems;

- budgetary provision has been made to ensure high availability;

- for reasons of high availability, and given that the system serves two different institutions, two VTC systems are foreseen, dimensioned for medium sized rooms, as it is envisaged that additional delegates may in certain cases be present for VTCs.

- the operational cost of two operators has been foreseen.

8. Regarding sites in Member States and other institutions:

- Budget provision has been made for cryptographic and hardware equipment for **three sites per Member State (President/Prime Minister, Ministry of Foreign Affairs and Permanent Representation to the EU),** and for up to **two sites each in the European Council/Council headquarters and the Commission and one for the EEAS. Additional systems may be considered for other EU Institutions, Bodies or Agencies (EUIBA) as necessary**.

- For each location, the costs of an IP encryptor up to SECRET UE / EU SECRET, VTC room equipment and installation are taken into account;

- A 'risk on cost' margin has been foreseen of 50% on equipment and 30% on services;

- Maintenance costs have been estimated based on current maintenance costs for the different types of equipment;

- Costs of security assessment visits to Member States have not been included;

- **As mentioned above, costs for building works and communication costs are not included; these costs must be borne by the member states and the institutions themselves**. These costs are dependent on the actual location offices selected by the member states, so no estimates on this can be provided.

- There will be a cost to the Council budget for some building works within the Council building in order to provide a suitable meeting facility for the President of the European Council. These cannot be quantified at this stage;

- In the current budget provisions, no funds are envisaged for including the permanent representations.

9. Regarding the accreditation process, the cost has been foreseen for delivering appropriate system documentation as required by the accreditation process, and the production of the Secure Operating Procedures and documentation.

10. As the system should be capable of relatively easy scaling, if needed, the possibility exists for Member States to purchase hardware to equip additional endpoints if deemed necessary.

Budgetary planning

11. The budget for the system as described would need to be foreseen in the Council budget for 2021 and 2022. The budget would be spread over 2021 and 2022 as follows:

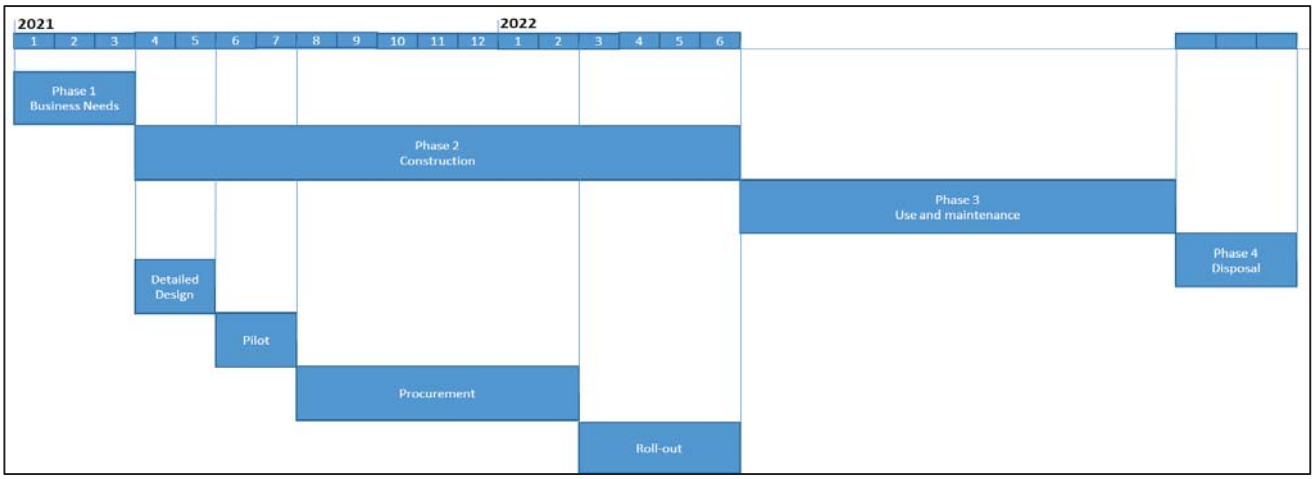
- 2021: expenditure for the central hub and accreditation process: 476.000 Euro; there will be an additional cost for some building works (to be quantified);

- 2022: equipping of sites in Member States, the Commission and the EEAS: 1.917.000 Euro.

12. An annual operating budget for operations of 409.200 Euro needs to be foreseen from 2022 onwards.

Planning

13. The figure below gives a high level overview of the planning of the service.



14. The project phase of the service is envisaged to take 18 months. This covers the first two phases as described in the Council's accreditation process (i.e. the development of business needs and the construction of a compliant CIS system).

15. The construction phase can be further broken down into four distinct activities, i.e.:

- Detailed design of the system. This activity will also include the security engineering and the System-specific Security Requirements Statements, although both documents may be further enhanced and iterated during the pilot;

- A pilot to make sure procurement of the system will result in an operational system, and to fine-tune the engineering design and the low level specifications.

- A procurement phase of 7 months allows for the procurement and delivery of the equipment. During this phase, it is also envisaged that the physical construction of the secure areas in the member States and institutions are executed.

- A roll-out phase of 4 months will enable to join all envisaged locations to the system.

It should be noted that this is an ambitious timetable requiring coordinated works across Member States. This coordination will be organised through the Council's Coordination Committee for CIS.

16. Phase 3 is the operation and maintenance of the system. It is expected that the system will have a lifetime of approximately 10 years, although technology updates of certain components might be necessary during this period.

17. At the end of its useful lifetime, the system and equipment will be decommissioned in accordance with the relevant security rules (phase 4).